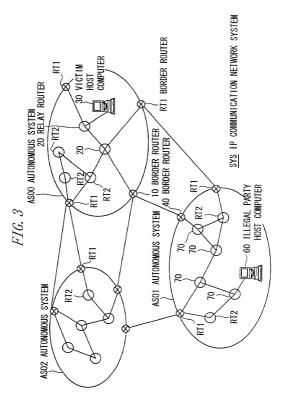


FIG. 2



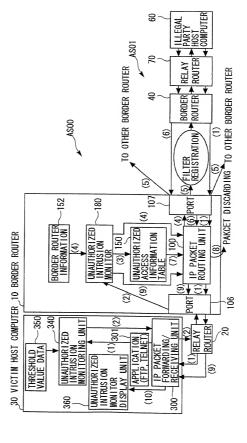
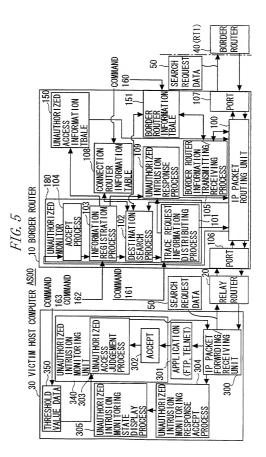


FIG. 4



50	
	SEARCH REQUEST DATA
	REQUEST TYPE
	(REGISTRATION/CANCELLATION)
	DESTINATION ROUTER IP ADDRESS
	SELF-ROUTER IP ADDRESS
	DESTINATION IP ADDRESS
	PROTOCOL TYPE
	PORT NUMBER

80	UNIAUTHODIZED AGGEGG INFORMATION
	UNAUTHORIZED ACCESS INFORMATION
`	MONITORING PERIOD (TIME)
	DESTINATION IP ADDRESS
	PROTOCOL TYPE
	PORT NUMBER

FIG. 8

350							
	THRESHOLD VALUE DATA						
	ICMP 50 TIMES/SEC (1)						
	TELNET 3 TIMES/SEC (1)						
	FTP 3 TIMES/SEC (1)						
	ICMP 80 TIMES/SEC (2)						
	FTP 3 TIMES/SEC (2)						
	! !						
	1						

152

BORE	DER RO	UTER	INFO	RMATION	
В0	RDER F	ROUTER	IP.	ADDRESS	#1
В0	RDER I	ROUTER	1P	ADDRESS	#2
В0	RDER I	ROUTER	IP.	ADDRESS	#3
ВО	RDER I	ROUTER	I I P	ADDRESS	#4
<u> </u>					
L					

- 90 CONNECTION ROUTER INFORMATION

SELF-ROUTER INFORMATION	CONNECTION ROUTER INFORMATION
MAC ADDRESS #1	CONNECTION ROUTER IP ADDRESS #1
VPI/VCI#1	CONNECTION ROUTER IP ADDRESS #2
INPUT PORT INFORMATION #1	CONNECTION ROUTER IP ADDRESS #3
1	I ADDRESS #5
1	!
	i
	!

120	UNAUTHORIZED PACKET INFORMATION
	DESTINATION IP ADDRESS
	PROTOCOL TYPE
	PORT NUMBER
	IP HEADER
	MAC ADDRESS OR VPI/VCI OR INPUT PORT INFORMATION

140 UNAUTHORIZED INTRUSION RESPONSE DATA

DESTINATION IP ADDRESS
SELF-ROUTER IP ADDRESS
PROTOCOL TYPE
PORT NUMBER
SELF-ROUTER AS NUMBER
RESPONSE TYPE (DISCOVERING OF UNAUTHORIZED ACCESS/MONITORING OF UNAUTHORIZED ACCESS)

350 JUDGEMENT TYPE OF THRESHOLD VALUE DATA

ICMP 50 TIMES/SEC (1) TELNET 3 TIMES/SEC (1) FTP 3 TIMES/SEC (1) ICMP 80 TIMES/SEC (2) FTP 3 TIMES/SEC (2)

ELEMENTS PER JUDGEMENT TYPE

ICMP 50 TIMES/SEC (1): JUDGED

TO BE UNAUTHORIZED ACCESS WHEN ALL THE FOLLOWING CONDITIONS ARE COINCIDENT WITH AND CONDITIONS UNAUTHORIZED 50 TIMES/SEC ACCESS TRY COUNT APPLICATION NO IDENTIFIER IDENTIFIER MESSAGE TYPE LCMP ECHO SAME USER JUDGEMENT NEGATED SAME SESSION NEGATED JUDGEMENT INPUT COMMAND NO COMMAND ALARM FUNCTION ALARMED MONITORING Al I START TIME MONITORING END TIME ALL TELNET 3 TIMES/SEC (1): JUDGED TO BE UNAUTHORIZED ACCESS WHEN ALL THE FOLLOWING CONDITIONS ARE COINCIDENT WITH AND CONDITIONS **UNAUTHORIZED ACCESS** 3 TIMES/SEC TRY COUNT APPLICATION TELNET IDENTIFIER MESSAGE TYPE NOTHING SAME SESSION JUDGED JUDGEMENT SAME USER JUDGEMENT JUDGED INPUT COMMAND

ALARM FUNCTION

MONITORING

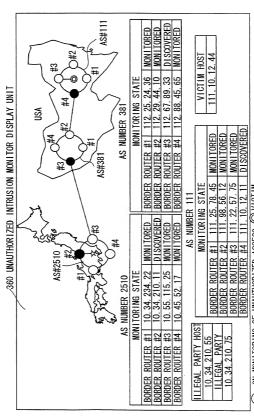
START TIME MONITORING END TIME PING

ALARMED

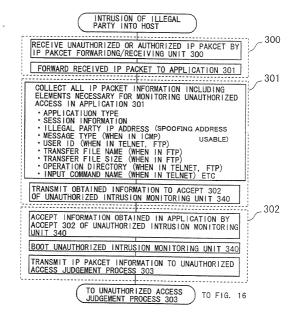
01:00

06:00





) ON-MONITORING OF UNAUTHORIZED ACCESS ◎ VICTIM DISCOVERING OF UNAUTHORIZED ACCESS ☆ ILLEGAL PARTY



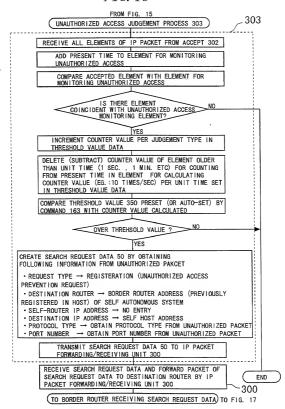
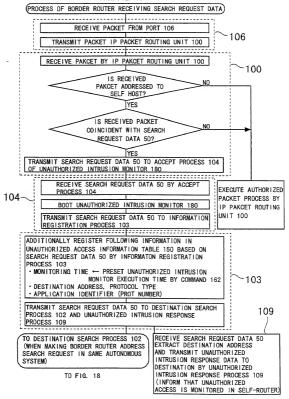


FIG. 17

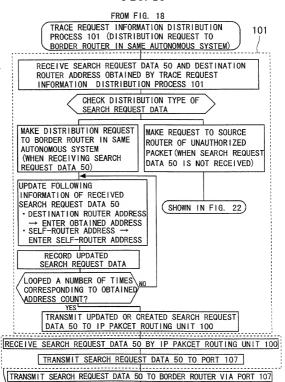


FROM FIG. 17 DESTINATION SEARCH PROCESS 102 102 (WHEN MAKING BORDER ROUTER ADDRESS SEARCH REQUEST IN SAME AUTONOMOUS SYSTEM -----RECEIVE SEARCH REQUEST DATA 50 OR UNAUTHORIZED PACKET INFORMATION BY DESTINATION SEARCH PROCESS 102 CHECK TYPE OF DESTINATION SEARCH MAKE BORDER ROUTER ADDRESS MAKE SOURCE ROUTER ADDRESS SEARCH REQUEST IN SAME SEARCH REQUEST OF AUTONOMOUS SYSTEM (WHEN UNAUTHORIZED PACKET (WHEN RECEIVING SEARCH REQUEST SEARCH REQUEST DATA 50 IS DATA 50) NOT RECEIVED) REFER TO BORDER ROUTER SHOWN IN FIG. 21 INFORMATION TABLE 151 REGISTERED BEFOREHAND BY COMMAND 160 AND OBTAIN ALL IP ADDRESSES OF DISTRIBUTE DESTINATIONS OF SEARCH REQUEST DATA 50 TRANSMIT OBTAINED BORDER ROUTER ADDRESS AND SEARCH REQUEST DATA 50 TO TRACE REQUEST INFORMATION DISTRIBUTION PROCESS 101

TO TRACE REQUEST INFORMATION DISTRIBUTION PROCESS 101 (DISTRIBUTION REQUEST TO BORDER ROUTER IN SAME AUTONOMOUS SYSTEM)

100

FIG. 19

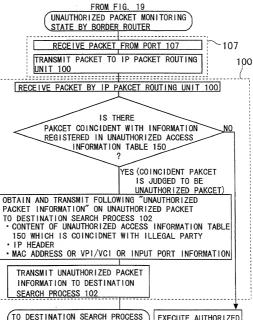


TO UNAUTHORIZED PACKET MONITORING

STATE BY BORDER ROUTER

107

TO FIG. 20



UNAUTHORIZED PACKET)
TO FIG. 21

102 (WHEN MAKING SOURCE ROUTER

ADDRESS SEARCH REQUEST OF

EXECUTE AUTHORIZED PACKET PROCESS BY IP PACKET ROUTING UNIT 100

DESTINATION SEARCH PROCESS 102 102 (WHEN MAKING SOURCE ROUTER ADDRESS SEARCH REQUEST OF UNAUTHORIZED PACKET) RECEIVE SEARCH REQUEST DATA 50 OR UNAUTHORIZED PACKET INFORMATION BY DESTINATION SEARCH PROCESS 102 CHECK TYPE OF DESTINATION SEARCH MAKE BORDER ROUTER ADDRESS MAKE SOURCE ROUTER ADDRESS SEARCH REQUEST IN SAME SEARCH REQUEST OF AUTONOMOUS SYSTEM (WHEN UNAUTHORIZED PACKET (WHEN RECEIVING SEARCH REQUEST SEARCH REQUEST DATA 50 IS NOT RECEIVED) (WHEN DATA 50) RECEIVING UNAUTHORIZED SHOWN IN FIG. 18 PACKET INFORMATION) TYPE OF RECEIPT VPI/CPI MAC ADDRESS INPUT PORT INFORMATION REFER TO CONNECTION ROUTER INFORMATION TABLE 108 REGISTERED WITH ADDRESS OF ROUTER CONNECTED TO ABOVE ROUTER BY COMMAND 160 AND OBTAIN ROUTER ADDRESS (SOURCE ADDRESS OF UNAUTHORIZED PACKET) CORRESPONDING TO INFORMATION RECEIVED TRANSMIT OBTAINED SOURCE ADDRESS OF UNAUTHORIZED

TO TRACE REQUEST INFORMATION DISTRIBUTION PROCESS 101 (WHEN MAKING REQUEST TO SOURCE ROUTER OF UNAUTHORIZED PACKET)

PACKET AND UNAUTHORIZED PACKET INFORMATION TO TRACE REQUEST INFORMATION DISTRIBUTION PROCESS 101

FIG 22 FROM FIG. 21

TRACE REQUEST INFORMATION DISTRIBUTION

PROCESS 101 (WHEN MAKING REQUEST TO SOURCE ROUTER OF UNAUTHORIZED PACKET) -----

RECEIVE UNAUTHORIZED PACKET INFORMATION AND DESTINATION ROUTER ADDRESS OBTAINED BY TRACE REQUEST INFORMATION DISTRIBUTION PROCESS 101

> CHECK TYPE OF DISTRIBUTION OF SEARCH REQUEST DATA

MAKE DISTRIBUTION REQUEST TO BORDER ROUTER IN SAME AUTONOMOUS SYSTEM (WHEN RECEIVING SEARCH REQUEST DATA 50)

MAKE REQUEST TO SOURCE ROUTER OF UNAUTHORIZED PACKET (WHEN SEARCH REQUEST DATA 50 IS NOT RECEVIED) (WHEN RECEIVING UNAUTHORIZED PACKET INFORMATION)

101

SHOWN IN FIG. 19

CREATE SEARCH REQUEST DATA 50 BASED ON FOLLOWING INFORMATION

- REQUEST TYPE→ENTER REGISTRATION (UNAUTHORIZED ACCESS PREVENTION REQUEST)
- DESTINATION ROUTER ADDRESS→OBTAINED BY
- DESTIANTION SEARCH PROCESS 102 - SELF-ROUTER ADDRESS→ENTER SELF-ROUTER ADDRESS
- DESTINATION IP ADDRESS→OBTAINED FROM UNAUTHORIZED PACKET INFORMATION
- PROTOCOL TYPE→OBTAINED FROM UNAUTHORIZED PACKET INFORMATION

PORT NUMBER → OBTAINED FROM UNAUTHORIZED PAKCET

TRANSMIT UPDATED OR CREATED SEARCH REQUEST DATA 50 TO IP PACKET ROUTING PROCESS 100 AND UNAUTHORIZED INTRUSION RESPONSE PROCESS 109

......... RECEIVE SEARCH REQUEST DATA 50 BY IP PAKCET ROUTING PROCESS 100

TRANSMIT SEARCH REQUEST DATA 50 TO PORT 107

TRASMIT SEARCH REQUEST DATA 50 TO BORDER ROUTER VIA PORT 107

TO BORDER ROUTER RECEIVING SEARCH REQUEST DATA (REPEATED) RECEIVE SEARCH REQUEST DATA 50 EXTRACT DESTINATION ADDRESS AND TRANSMIT UNAUTHORIZED INTRUSION RESPONSE DATA TO DESTINATION BY UNAUTHORIZED INTRUSION RESPONSE PROCESS 109 (INFORM THAT UNAUTHORIZED INTRUSION IS DISCOVERED IN SELF-ROUTER)

-107

~100

TO FIG. 17